Ecrit par Echo du Mardi le 15 août 2022

Télétravail en vacances, comment protéger vos données



Les Tracances, la nouvelle tendance du télétravail en vacances. D'après une enquête menée par le cabinet Génie des lieux et publiée le 11 juillet dernier, 35 % des travailleurs français déclarent qu'ils feront du télétravail depuis leur lieu de vacances cet été. Parmi eux, 24 % se limiteront à 1 ou 2 jours par semaine afin de profiter de leurs proches, tandis que 11 % le feront à temps plein.

Voyager tout en travaillant, c'est pouvoir changer de bureau chaque jour, profiter de paysages d'exception pendant sa pause-café mais aussi s'exposer à des risques en matière de cybersécurité. Pour partir tranquille, en plus de penser à prendre l'anti-moustique dans la valise, le digital nomad doit veiller à la protection de ses données.

Eviter de se connecter depuis un lieu public

Loin du bureau, le digital nomad doit éviter de se connecter en Wi-Fi dans un lieu public complètement

Ecrit par Echo du Mardi le 15 août 2022

ouvert comme une gare ou un café. Ces réseaux comportent de multiples failles de sécurité. Celles-ci peuvent entraîner une fuite des données contenues dans l'ordinateur, dont celles stockées sur le réseau de l'entreprise et qui sont souvent confidentielles. Cela revient à laisser la porte grande ouverte à des intrusions malveillantes. Il en est de même dans les espaces de coworking. Même s'ils paraissent plus sécurisés, les connexions dans ces lieux ne bénéficient généralement pas d'un niveau de sécurité suffisant. De plus, le digital nomad s'expose à des risques de vol ou perte de matériel (disque dur, clé USB…), qui pourraient compromettre gravement la sécurité des données.

Utiliser des équipements fiables
Il est déconseillé d'utiliser un équipement personnel pour travailler. En effet, ce dernier n'a pas bénéficié des configurations de sécurité nécessaires : authentification au démarrage, chiffrement des disques, gestion des droits administrateurs ou de la connexion à des supports amovibles… Ces contrôles doivent être effectués par l'entreprise sur l'équipement professionnel avant de laisser partir le digital nomad, que ce soit à l'étranger ou dans sa maison de campagne. Objectif : protéger les accès aux données.

Préserver la confidentialité des échanges
Le digital nomad entretient des liens constants avec son entreprise. Pour cela, il utilise des outils de visioconférence pour ses réunions, ses appels et aussi ses partages de fichiers. Là encore, la vigilance est de mise. Des protections physiques peuvent être utiles, comme des filtres écrans ou des verrous de ports USB qui empêchent tout regard indiscret ou intrusion dans le système. Aujourd'hui, la plupart des échanges en vidéoconférence sont susceptibles d'être écoutés et regardés. En dehors du bureau, ce risque d'espionnage informatique est encore plus élevé. Il peut entraîner des conséquences graves pour l'intégrité des salariés et des données de l'entreprise. Les entreprises ont donc intérêt à faire le choix d'une solution de visio collaboration sécurisée.

Vous avez dit cyber sécurité ?
L'ANSSI les accompagne dans leur choix via un processus de certification et de qualification. Elle identifie ainsi les solutions de cybersécurité les plus fiables, en leur attribuant un label « Visa de sécurité ».

VPN oui, mais pas que…
Ne pas se contenter de l'utilisation d'un VPN : Le VPN constitue un lien sécurisé entre l'équipement du salarié en voyage et le réseau de son entreprise. Mais il ne protège pas des failles de sécurité. Si le télétravailleur se connecte à un réseau Wi-Fi public et laisse entrer par mégarde un logiciel malveillant sur son ordinateur, le virus pourra s'infiltrer via le VPN et remonter jusqu'au serveur de l'entreprise…

Prendre garde à ses propres données personnelles
Qui dit digital nomad dit passeport, billets d'avion ou de trains qui sont parfois partagés dans les messageries des outils de visiocollaboration. Ces données personnelles sont exposées si les échanges ne sont pas sécurisés, ce qui peut entraîner une usurpation d'identité.

Sources
Cet article provient de Tixeo secure video conferencing. D'après une enquête **menée par le cabinet**

Ecrit par Echo du Mardi le 15 août 2022

Génie des lieux et publiée le 11 juillet dernier. Renaud Ghia, Président de Tixeo, le leader européen de la visioconférence sécurisée et l'unique technologie de visioconférence à être certifiée et qualifiée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), a offert ces conseils.
MH



DR